



WORKPLACE LAW REPORT



Reproduced with permission from Workplace Law Report, 7 WLR 1557, 11/20/2009. Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

TECHNOLOGY

Employers increasingly are turning to the Computer Fraud and Abuse Act, initially intended to deter hackers and protect data on federal computers, to obtain injunctive and monetary relief against employees accused of using company computers to defraud the employer, particularly where noncompetition agreements or trade secrets are involved. Attorney Adam Augustine Carter of the Employment Law Group explores the CFAA and court decisions interpreting the act, and suggests strategies employees can use to avoid CFAA claims and to defend against them.

Combating Claims of Computer Fraud and Abuse

By ADAM AUGUSTINE CARTER*

** Adam Augustine Carter is a principal at the Employment Law Group law firm in Washington, D.C., where he represents individuals in employment disputes, including litigation on the Computer Fraud and Abuse Act. The author thanks Tadena Simpson, a legal assistant at the Employment Law Group law firm and law student in the class of 2011 from George Mason University, for her contributions to this article.*

The Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, was originally enacted in 1984 as a criminal statute to deter hackers and protect data on federal computers. Over time, the scope of the CFAA evolved to include a private right of action for any person who suffers damage or loss because of a violation of the CFAA. Not surprisingly, employers have increasingly taken advantage of the CFAA’s civil remedies to obtain both injunctive and monetary relief against employees, making the federal statute a potent weapon against employees, especially in the context of noncompete and trade secrets litigation. This article examines the CFAA and suggests strategies that an employee can consider when fighting against a CFAA lawsuit.

I. Elements of a CFAA Claim

To establish a civil action against an employee under the CFAA, an employer must prove that the employee: (1) “knowingly and with the intent to defraud,” (2) accessed a “protected computer,” (3) “without authorization,” and as a result (4) caused a damage or loss of at least \$5,000.¹ This analysis focuses primarily on the last two elements and the extent to which a former employee has damaged or compromised the integrity of the employer’s computer system.

An employer does not have a cause of action under the CFAA if the alleged misconduct does not involve conduct prohibited by the act. Violations include but are not limited to:

1. damage to a protected computer that results in a loss of at least \$5,000;
2. the impairment of a medical examination, diagnosis, treatment or care of an individual;
3. physical injury to a person; and
4. threats to public health or safety.

A. What Is a “Protected Computer” Under the CFAA? A “protected computer” is defined broadly to include any computer that is “used in interstate or foreign commerce or communication.”² This includes any computer connected to the internet.³

B. Did the Employee Have Authorization to Access the Protected Computer? The key element to any CFAA claim is the employee’s unauthorized access to the employer’s computer system. Accordingly, an employer does not have a cause of action under the CFAA if access to the part of the employer’s computer system that the employee allegedly accessed was never revoked.⁴ The line blurs, however, when an employee planning to leave her job and while still employed and still authorized to use her employer’s computer system, uses that system for purposes adverse to the employer’s interest, for example, if the employee gathers and disseminates information for competitive purposes. Some courts have addressed this issue by treating such conduct as “exceeding authorized access,” while others have ruled that an employee’s authorization to access ends the moment he or she acts contrary to the employer’s interest, thereby rendering the conduct as one “without authorization.”⁵ Still others have determined that such conduct

is outside the scope of the act.⁶ A review of recent case law reveals the various conclusions that courts have reached in analyzing this particular element of the CFAA.

In *International Airport Centers, LLC v. Citrin*, the Seventh Circuit ruled in favor of a real estate agency on its claims for violations of the CFAA.⁷ In *Citrin*, the employee deleted files from his company-issued laptop and installed a secure-erasure program making it impossible for the agency to recover any of the deleted information.⁸ According to the employee, there was no basis for the CFAA claim because he was “authorized” to access his computer at the time he deleted the files.⁹ The Seventh Circuit rejected this argument, finding that “[an employee’s] breach of his duty of loyalty [in deleting relevant files] terminate[s] his agency relationship. . . and with it his authority to access the [company] laptop.”¹⁰ The Seventh Circuit concluded that an employee’s authorized access terminates when the employee’s mental state changes from loyal employee to disloyal competitor and the employee accesses his employer’s computer for an unauthorized purpose, i.e., to defraud or cause harm to the former employer.¹¹

Other courts, however, have considered and emphatically rejected the agency law notion of authorization applied in *Citrin*. For example, in *International Ass’n of Machinists & Aerospace Workers v. Werner-Masuda*,¹² the court held that the employer could not state a claim for relief under the CFAA because “[the employee’s] access had not been revoked.”¹³ According to the *Werner-Masuda* court, Congress intended for the statute to apply to outside computer hackers and not to disloyal employees who access their employer’s computer system on behalf of the employer’s competitor.¹⁴ Further, the court concluded that the CFAA expressly prohibits “unauthorized access” and not “unauthorized disclosure” of information.¹⁵ A Texas court reached a similar result

administrative assistant exceeded her authority by installing data shredding software causing permanent deletion of financial records on company’s computer).

⁶ See *B & B Microscopes v. Armogida*, 532 F. Supp. 2d 744 (W.D. Pa. 2007) (court held that because CFAA delineates between authorized and unauthorized access, reading of statute that once employee begins violating duty of loyalty to his employer any authorized access is withdrawn, would render the CFAA’s distinction meaningless); see also *Lockheed Martin Corp. v. Speed*, No. 6:05-CV-1580-ORL-31, 2009 WL 2683058, at *4 (M.D. Fla. Aug. 1, 2006) (court refused to recognize CFAA claim where employer permitted its employees, as a function of their respective positions, to access the precise information at issue on ground that “Congress chose not to reach. . . those [employees] with access authorization.”); *Black & Decker Inc. v. Smith*, No. 07-1201, 2008 WL 3850825, at *3 (W.D. Tenn. Aug. 13, 2008) (court concluded that “the [CFAA] targets the unauthorized procurement or alteration of information, not its misuse.”).

⁷ *Citrin*, 440 F.3d at 421.

⁸ *Id.* at 419.

⁹ *Id.* at 421.

¹⁰ *Id.* at 420–21.

¹¹ *Id.* at 421.

¹² *Int’l Ass’n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479 (D. Md. 2005).

¹³ *Id.* at 499.

¹⁴ *Id.* at 498.

¹⁵ *Id.* at 499.

¹ 18 U.S.C. § 1030(a)(4); see also *Pacific Aerospace & Elecs. Inc. v. Taylor*, 285 F. Supp. 2d 1188, 1195 (E.D. Wash. 2003).

² 18 U.S.C. § 1030(e)(2)(B).

³ See *Cont’l Group Inc. v. KW Prop. Mgmt. LLC*, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009) (court held that connection to internet is “affecting interstate commerce or communication” and thus, computers connected to internet are protected under CFAA).

⁴ See *LVRC Holdings v. Brekka*, 581 F.3d 1127, 29 IER Cases 1153 (9th Cir. 2009); 2009 WL 2928952 (court held that employee uses computer “without authorization” when person has not received permission “to use computer for any purpose . . . or when the employer has rescinded permission to access the computer and the [employee] uses the computer anyway”).

⁵ *Int’l Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); 4 WLR 329, 3/17/06, (court held that “authorized access” ends when employee breaches his duty of loyalty); *Patrick Patterson Custom Homes Inc. v. Bach*, 586 F. Supp. 2d 1026, 1034-35 (N.D. Ill. 2008) (court held that employer stated cause of action for violation of CFAA because it alleged that its

in *Bridal Expo Inc. v. Van Florestein*¹⁶ when it concluded that defendants, former employees of the bridal exposition company Bridal Expo, did not copy information from the company's computers "without authorization" even though one of the former employees admitted to downloading Bridal Expo's database and later, used the downloaded information for improper purposes.¹⁷ According to the court, "if Congress wanted to reach all wrong doers who access information that they will use to the detriment of their employers, it could have omitted the limiting words on authorization altogether."¹⁸ Thus, finding that the former employees had signed no confidentiality agreement with Bridal Expo or any other agreement restricting their access to the files they had been working with at their jobs at Bridal Expo, the court denied the CFAA claim.¹⁹

In the most recent case to tackle this issue, *LVRC Holdings LLC v. Brekka*,²⁰ the Ninth Circuit also rejected the agency law notion of authorization applied in *Citrin*. In *Brekka*, the Ninth Circuit held that a marketing consultant did not violate the CFAA because he did not access the employer's computer "without authorization" when he allegedly e-mailed his employer's documents to himself and to his wife to further his own competing business.²¹ In reaching its decision, the Ninth Circuit concluded that "[n]o language in the CFAA supports the argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest."²² Instead, "[an employee] uses a computer 'without authorization' when the person has not received permission to use the computer for any purpose . . . or when the employer has rescinded permission to access the computer and the [employee] uses the computer anyway."²³

The *Brekka* court also held an employee remains authorized to use the protected computer even when an agreement subjects the employee's access to certain limitations and the employee violates these limitations.²⁴

While many courts have sided with the *Werner-Masuda* court, the scope of the term "authorization" remains unresolved.²⁵ Even so, courts are more likely to

¹⁶ *Bridal Expo Inc. v. Van Florestein*, No. 4:08-CV-03777, 2009 WL 255862 (S.D. Tex. 2009).

¹⁷ *Bridal Expo*, 2009 WL 255862, at *11.

¹⁸ *Id.* at *10.

¹⁹ *Id.* at *11.

²⁰ 581 F.3d 1127, 29 IER Cases 1153, 2009 WL 2928952 (9th Cir. 2009).

²¹ *Brekka*, at *6-7.

²² *Id.* at *5.

²³ *Id.* at *7; see also *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008) (employee's acquisition of employer's confidential information prior to resigning for new position with employer's competitor was not "without authorization" or in matter that "exceeded authorized access" where employee was permitted to view specific files he allegedly e-mailed himself).

²⁴ *Brekka*, at *5 ("It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'").

²⁵ Compare *Brekka*, at *5 (former employee who e-mailed sensitive company documents that he accessed with permission to his personal computer did not exceed his authorized access, even if he planned to use those documents to further his own business objectives) and *Jet One Group Inc. v. Halcyon Jet Holdings*, No. 08cv3980, 2009 WL 2524864, *5-6

dismiss a CFAA claim where an employee's counsel can prove that the alleged "access" was harmless, was not for an improper purpose, or that the employee accessed the former employer's computer system for legitimate, work-related reasons.²⁶ Moreover, a court is less likely to consider a CFAA claim against an employee where the employee's unauthorized conduct did not produce "anything of value."²⁷

C. What Constitutes Loss or Damage for a Viable CFAA Claim? To be actionable, a CFAA claim must also allege that the employee's wrongful conduct resulted in a \$5,000 damage or loss to the employer. Failure of proof on this element is "fatal" to a CFAA cause of action.²⁸ Thus, employees should always try to challenge an employer's complaint by arguing that his or her conduct did not result in a "loss" to the employer.

1. "Loss" Under the CFAA. In determining what constitutes a "loss" under the CFAA, courts have consistently interpreted "loss" to mean expenses related to restoring computer data, fixing actual damages to a computer system and modifying a computer system to preclude further data transfer.²⁹ Courts disagree, how-

(E.D.N.Y. Aug. 14 2009) (dismissing complaint claiming that defendants, who were permitted to access client lists in question in normal course of business even when defendants later used those client lists to compete against plaintiff) with *Int'l Airport*, 440 F.3d at 420 (employee's misappropriation of confidential information violated his duty of loyalty, thereby "terminating his agency relationship . . . and with it his authority to access the laptop") and *Calyon*, No. 07 Civ. 2241, 2007 WL 2618658 at *1 (holding that employees who copied their employer's proprietary electronic documents before their termination must have known doing so was "in contravention of the wishes and interests of the employer" and therefore exceeded the scope of their authorized access).

²⁶ *Hecht v. Components Int'l Inc.*, 867 N.Y.S.2d 889 (2008) (court granted summary judgment dismissing CFAA counterclaim where employee's access to company's e-mail server was "standard" suggesting that "sensitive information was not reached"); *Lockheed Martin*, 2006 WL 2683058, at *8 ("The copying of information from a computer onto a CD or PDA is a relatively common function that typically does not, by itself, cause permanent deletion of the original computer files. In the absence of an allegation of permanent deletion or removal, the Court will not create one."); *Resdev LLC v. Lot Builder Ass'n Inc.*, No. 6:04-CV-1374ORL31DAB, 2005 WL 1924743, at *4-5 (M.D. Fla. 2005) (Court held that to have "damage" under the CFAA, there must be "some diminution in the completeness or useability of the data or information on a computer system." Determination of whether damage exists hinges on physical change in data, program, system, or information).

²⁷ *United States v. Czubinski*, 106 F.3d 1069, 1070 (1st Cir. 1997) (employee of IRS did not violate CFAA even though he knowingly disregarded IRS confidential information rules by performing searches outside scope of his contract representative duties to satisfy his own curiosity about tax information of friends, political rivals, and acquaintances, because there was no evidence that he printed out, recorded, or used information he read to obtain "anything of value"); see also *P.C. Yonkers Inc. v. Celebrations the Party & Seasonal Superstore LLC.*, 428 F.3d 504, 505 (3rd Cir. 2005); *In re America Online Inc.*, 168 F. Supp. 2d 1359, 1360 (S.D. Fla. 2001).

²⁸ *Pearl Investments LLC v. Standard I/O Inc.*, 257 F. Supp. 2d 326, 349 (D. Me. 2003).

²⁹ See *Lasco Foods Inc. v. Hall & Shaw Sales, Marketing & Consulting LLC*, No. 4:08CV01683, 2009 WL 151687, at *5 (E.D. Mo. 2009) ("[c]ourts have consistently interpreted loss . . . to mean a cost of investigating or remedying damage to a computer, or a cost incurred because the computer's ser-

ever, on whether consequential damages, such as loss in the value of trade secrets or competitive advantage constitute a “loss” under the CFAA.³⁰

In *Civic Center Motors Ltd. v. Mason Street Import Cars Ltd.*,³¹ for example, a New York court held that lost profits and wasted investments are not compensable losses under the CFAA.³² In *Civic Center*, a car dealership brought a CFAA claim against its competitor, seeking compensation for their “now wasted investment” in a customer database and lost profits resulting from its competitor’s unfair competitive edge.³³ The court refused to recognize Civic Center’s claims, concluding that “losses under the CFAA are compensable only when they are the result from damage to, or inoperability of, the accessed computer system.”³⁴ Finding that the former employees’ access to the dealership’s web-based database did not affect the integrity of the database’s information, the court dismissed the CFAA claim.³⁵

The court in *Nexans Wires S.A. v. Sark-USA Inc.*,³⁶ reiterated the court’s position in *Civic Center* when it rejected an employer’s CFAA claim seeking reimbursement for the cost of flying two executives from Germany to New York to meet and discuss the consequences of their competitor’s gain in competitive edge from their use of unlawfully gained information.³⁷ In reaching its decision, the court pointed to the fact that the executives’ trip and subsequent meetings were unrelated to “investigating or remedying damage to a computer,” and therefore, fell outside the definition of

vice was interrupted.”); *Forge Indus. Staffing Inc. v. De La Fuente*, No. 06 C 3848, 2006 WL 2982139, at *6-7 (N.D. Ill. 2006) (loss includes cost of hiring forensic computer expert to recover destroyed data in addition to actual damages to computer system); see also *Matter of Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001) (court noted that “Congress intended the term ‘loss’ to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker.”); 18 U.S.C. § 1030(e)(11) (loss is defined as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred or other consequential damages incurred because of interruption of service.”).

³⁰ *Compare Garelli Wong & Associates Inc. v. Nichols*, 551 F. Supp. 2d 704 (N.D. Ill. 2008) (court ruled that copying or misappropriation of trade secret through use of computer does not, on its own, constitute “damage” under CFAA) with *HUB Group, Inc. v. Clancy*, No. Civ. A. 05-2046, 2006 WL 208684, at *3-4 (E.D. Pa. 2006) (employee exceeded scope of his authorization into former employer’s database when he took information to use as TTS employee) and *Caylon*, No. 07 Civ. 2241, 2007 WL 2618658 at*1 (S.D.N.Y. Sept. 5, 2007) (holding that employees who copied their employer’s proprietary electronic documents before their termination must have known doing so was “in contravention of the wishes and interests of the employer” and therefore exceeded scope of their authorized access).

³¹ *Civic Ctr. Motors Ltd. v. Mason St. Import Cars Ltd.*, 387 F. Supp. 2d 378 (S.D.N.Y. 2005).

³² *Id.* at 381.

³³ *Id.* at 382.

³⁴ *Id.* at 381.

³⁵ *Id.*

³⁶ *Nexans Wires S.A. v. Sark-USA Inc.*, 319 F. Supp. 2d 468 (S.D.N.Y. 2004).

³⁷ *Id.* at 476.

a recoverable “loss” under the statute.³⁸ According to the court, “[g]eneral non-computer costs incurred in investigating the violation [are] too far outside of the scope of the [CFAA].”³⁹ Other courts, however, have taken a broader view, suggesting that items such as misappropriated property, loss of goodwill, and investigative costs can be used to establish the “loss” requirement of a civil CFAA action.⁴⁰

In *EF Cultural Travel BV v. Explorica Inc.*,⁴¹ for example, the First Circuit held that the CFAA covered more than the losses directly attributed to the actual physical damage of a computer’s hard drive.⁴² Here, a tour company sued its competitor under the CFAA for allegedly using a “scraper” software program to glean prices from its website.⁴³ The company claimed that it sustained a compensable loss because it had to pay consultants to assess the effect of Explorica’s interference with its website.⁴⁴ In response, Explorica argued that it could not be liable under the CFAA because “their actions neither caused any physical damage nor placed any stress on EF’s website.”⁴⁵ The court rejected Explorica’s arguments, holding that “a general understanding of the word ‘loss’ would fairly encompass a loss of business, goodwill, and the cost of diagnostic measures” that a company takes to access the damage to its computer system.⁴⁶ According to the court, any losses stemming from an employee’s unauthorized conduct are recoverable, so long as it results in a loss of at least \$5,000.⁴⁷

2. “Damage” Under the CFAA. Under the statute, “damage” includes any “impairment to the integrity or availability of data, a program, a system or information.”⁴⁸ Some courts have ruled that the misappropriation of trade secrets does not constitute damages under the CFAA.⁴⁹ Others have ruled that the “damage” re-

³⁸ *Id.* at 473.

³⁹ *Id.* at 476.

⁴⁰ *Cont’l Group Inc. v. KW Prop. Mgmt. LLC*, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009); *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930 (9th Cir. 2004).

⁴¹ *EF Cultural Travel BV EF v. Explorica Inc.*, 274 F.3d 577 (1st Cir. 2001).

⁴² *Id.* at 585.

⁴³ *Id.* at 579.

⁴⁴ *Id.* at 580.

⁴⁵ *Id.* at 584.

⁴⁶ *Id.*; see also *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004) (court held that loss of business and business goodwill are economic damages under CFAA).

⁴⁷ *Explorica*, 274 F.3d at 585 (court held that \$20,000 that EF spent to determine whether its website had been compromised met \$5,000 threshold for loss or damage under CFAA).

⁴⁸ 18 U.S.C. § 1030(e)(8).

⁴⁹ See, e.g., *Garelli Wong & Assocs. Inc. v. Nichols*, 551 F. Supp. 2d 704 (N.D. Ill. 2008) (court ruled that copying or misappropriation of trade secret through use of computer alone does not constitute “damage” under CFAA); *Lockheed Martin*, 2006 WL 2683058, at *4 (copying of confidential data does not constitute “damage” under the CFAA); *Resdev*, 2005 WL 1924743, at *5 n.3 (noting that “damage” contemplates “some diminution in the completeness or useability of data or information on a computer system.”); *Davis v. Afilias Ltd.*, 293 F. Supp. 2d 1265 (M.D. Fla. 2003) (registry operator was not entitled to summary judgment on its counterclaim that employee that individual violated CFAA by using authorization codes to register domain names because World Intellectual Property Organization gave individual authorization codes to

quirement can be satisfied when the misappropriation is coupled with other harm.⁵⁰ Finally, there is authority that establishes the proposition that the misappropriation of trade secrets or confidential information alone is sufficient to establish the \$5,000 jurisdictional threshold.⁵¹

In *Shurgard Storage Centers Inc. v. Safeguard Self-Storage Inc.*,⁵² for example, the court held that even though the plaintiff's data was not physically erased or changed, the misappropriation of the trade secrets constituted an impairment to the integrity of the data in question and thus, fell within the definition of damage.⁵³ The majority of courts, however, have held that the misappropriation of trade secrets does not constitute damages under the CFAA.⁵⁴ According to one court, the absence of evidence that a computer network was damaged in any quantifiable amount by the alleged unauthorized access of the network precludes recovery under the CFAA.⁵⁵ Under this standard, a court likely will grant a motion to dismiss in a CFAA case where there is evidence that the misappropriated data remains intact on the employer's computer or the employer fails to plead impairment to the integrity or availability of data, a program, a system, or information.⁵⁶ Indeed, more courts are requiring employers to show computer-related losses, impairment of the original data, or a complete lack of permitted access.⁵⁷

register his names, which individual did through his registrar, there was no evidence that individual directly accessed registry operator's computer system to register domain names in question, and although it was discovered that codes were given to individual in error, individual could not be held simply on basis that he used codes to register domain names).

⁵⁰ *Black & Decker*, 568 F. Supp. 2d at 937 (W.D. Tenn. 2008) (misappropriating a trade secret coupled with other harm to the data constitutes "damage" under CFAA).

⁵¹ See e.g., *Four Seasons Hotel & Resorts BV v. Consorcio Barr SA*, 267 F. Supp. 2d 1268, 1324 (S.D. Fla. 2003).

⁵² *Shurgard Storage Centers Inc. v. Safeguard Self Storage*, 119 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000).

⁵³ *Id.*; see also 18 USC § 1030(e)(8)(A) (2000).

⁵⁴ *Id.* at 710; see also *Andritz v. S. Maint. Corp.*, 626 F. Supp. 2d 1264 (M.D. Ga. 2009); *Sam's Wines & Liquors Inc. v. Hartig*, No. 08 C 570, 2008 WL 4394962, at *3 (N.D. Ill. Sept. 24, 2008).

⁵⁵ See *Pearl Investments LLC v. Standard I/O Inc.*, 257 F. Supp. 2d 326, 349 (D. Me. 2003) (lack of evidence that computer network was damaged in any quantifiable amount by alleged unauthorized access by custom software company and its owners precluded developer's recovery under CFAA).

⁵⁶ See, e.g., *Garelli*, 551 F. Supp. 2d at 710 (court concluded that plaintiff failed to sufficiently plead damage under CFAA because misappropriation alone did not show "impairment to the integrity or availability of data, a program, a system, or information."); *Hartig*, 2008 WL 4394962, at *4 (court granted employee's 12(b)(6) motion to dismiss where employer failed to properly plead damage, i.e., impairment to integrity or availability of data, program, system, or information on its computer).

⁵⁷ See, e.g., *Condux Int'l v. Haugum*, No. 08-4824, 2008 WL 5244818, at *8 (D. Minn. 2008) (concludes that plain language of statute requires "some alteration of or diminution to the integrity, stability, or accessibility of the computer data itself" to be damage under CFAA); *P.C. Yonkers*, 428 F.2d at 513 (franchisees were not entitled to preliminary injunction where they demonstrated that former employee of their franchisor accessed computer system and did not show any information was taken; absent something more than mere access, franchisees could not succeed on their claim).

The lesson to be gleaned from these cases is that each case will turn on its own facts and the determination of whether the employer has sufficiently pleaded "damage" or "loss" will, among other things, be determined by the jurisdiction overseeing the case.

II. General Tips for Avoiding CFAA Claims

The computer equipment provided by an employer does not belong to an employee. Thus, an employee should return all computerized information to the employer upon departure and refrain from deleting or transferring any information from the company's computer system to a personal disk or e-mail without the company's express consent.

III. General Tips for Defending Against CFAA Claims

A. Challenge Reliability of Employer's Investigation. An employee should consider attacking the quality and reliability of the former employer's investigation into the employee's "access" by demonstrating that the former employer's methods for collecting evidence was unreliable or defective.⁵⁸

B. Challenge Any Injunctions That Are Broad or Contrary to Public Policy. Injunctions are an extraordinary remedy, which in the context of CFAA litigation can stifle competition and punish employees who may have inadvertently retained the former employer's documents. Accordingly, an employee should object to the entry of an injunction that is considerably broader than that which could ordinarily be obtained under a trade secrets or unfair competition theory.

C. Argue That There Was No Practice, Procedure or Policy Prohibiting "Improper" Access or Use of the Company's Documents. In the absence of a promulgated policy or practice prohibiting employees from the "improper" access or use of an employer's confidential information, a court likely will not find an employee's allegedly improper access of company documents to be in violation of the CFAA.⁵⁹

In *Brekka*, the Ninth Circuit held that an employer could not maintain its CFAA claim against a former employee accused of e-mailing company documents to his personal e-mail account because the employer could not establish that the former employee accessed its computer system "in excess of authorization" or "without authorization."⁶⁰ In reaching its decision, the court pointed to the fact that the employer failed to provide notice or employee guidelines distinguishing the proper and authorized use of employer information from the improper and unauthorized use of the company information in question.⁶¹ According to the Ninth Circuit, because Section 1030 is primarily a criminal statute and creates criminal liability for violators of the statute, the rule of lenity, which is rooted in considerations of no-

⁵⁸ *Brekka*, 2009 WL 2928952, at *8 (CFAA claim against employee failed because of contradictory evidence between the employer's own witness and expert evidence).

⁵⁹ *Id.* at *6.

⁶⁰ *Id.* at *1.

⁶¹ *Id.* at *6.

tice, applies.⁶² Thus, “no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed.”⁶³ In short, a court will likely not recognize a CFAA claim where an employee “would have no reason to know that making personal use of the company computer . . . would constitute a criminal violation of the CFAA.”⁶⁴

D. Assert the “Unclean Hands” Defense. To challenge an employer’s CFAA claims, an employee can rely on the “unclean hands” doctrine. According to this doctrine, “he who asks equity must do equity, and he who comes into equity must come with clean hands.”⁶⁵ In the context of CFAA litigation, this doctrine provides that “one who has acted in bad faith . . . or [has] been guilty of fraud, injustice or unfairness will appeal in

⁶² *Id.* at *6

⁶³ *Id.* at *6 (quoting *United States v. Santos*, 128 S. Ct. 2020, 2025 (2008)).

⁶⁴ *Id.*

⁶⁵ *Albert v. Albert*, 38 Va. App. 284, 299 (2002) (citing *Walker v. Henderson*, 151 Va. 913, 927-28 (1928)).

vain to a court of conscience.”⁶⁶ Thus, a court may not recognize a CFAA claim where there is evidence demonstrating that the employer engaged in wrongful or inequitable conduct with respect to the matter in litigation, i.e., the employer deleted all data that evidenced its retaliatory intent in filing the CFAA action.⁶⁷

IV. Conclusion

In sum, an employee faced with a lawsuit for violations of the CFAA has options to challenge the CFAA action, including the rule of lenity. Like lawsuits to enforce noncompetition provisions, CFAA actions are typically accompanied by a motion for a preliminary injunction or a motion for a temporary restraining order, which can put an employee out of work. Thus, it is critical quickly to assess and apply options available to the employee to gain the upper hand in the litigation and to avoid costs and being put on the defensive.

⁶⁶ *Matter of Garfinkle*, 672 F.2d 1340, 1346, n. 7 (11th Cir. 1982) (quoting *Peninsula Land Co. v. Howard*, 6 So. 2d 384, 389 (Fla. 1941)).

⁶⁷ *Cont'l Group Inc.*, 622 F. Supp. 2d at 1377.